

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Sean R. Crawford, a Special Agent with the Department of Homeland Security, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this Affidavit in support of an application under Federal Rule of Criminal Procedure 41 for a warrant to search three cellular phones, found during the arrest of GERBER VASQUEZ-BARRIOS and currently in law enforcement possession, and to seize fruits, evidence and/or instrumentalities of the specified federal offenses, to wit; 18 U.S.C. § 2251 (production of child pornography) and 18 U.S.C. § 2252(a)(4)(B) (possession of child pornography). The three cellular phones, further described in Attachments A.1, A.2, and A.3, are as follows: (1) a black Samsung Galaxy S5 (Model SM-G900A), (2) a gold Samsung Galaxy S7 (IMEI 359754071653702), and (3) a black Apple iPhone (IMEI 358689094665260) (“SUBJECT DEVICES”). There is probable cause to believe that, on the SUBJECT DEVICES, at the time of the execution of the search warrant, there will be the items, materials and objects described in Attachment B.

2. The statements made in this affidavit are made based on my personal observations and investigation, as well as information communicated or reported to me during the investigation by other participants in the investigation. In addition, the information contained herein does not include every fact known to agents.

3. I am a Special Agent employed by the United States Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations (“HSI”), assigned to the Office of the Resident Agent in Charge (“RAC”), Allentown, Pennsylvania. I have been employed in such capacity since March 2021. Prior to becoming a Special Agent with

HSI, I was a Patrol Agent with Customs and Border Protection from September 2009 until March 2021. I have completed the Criminal Investigator Training Program, as well as the HSI Special Agent Training at the Federal Law Enforcement Training Center in Glynco, Georgia. As an HSI Special Agent, I have experience conducting criminal investigations into violations of federal law. Prior to my current assignment, I was assigned to the HSI Philadelphia National Security Group. I have investigated and assisted with the investigation of numerous cases involving, but not limited to, human trafficking, child exploitation, importation violations, and controlled substance violations.

4. During my time as a law enforcement officer, I have participated in criminal investigations which involved the use of premises search warrants, electronic device search warrants, electronic mail search warrants, cell site and GPS location warrants, the review of telephone and email records, and covert surveillance. I have executed arrest warrants and served search warrants on residences, vehicles, storage mediums, and electronic devices. As a result of my training and experience, I am familiar with the techniques and methods of operations used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities.

5. I am an investigator or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered to conduct investigations of, and to make arrests for, the offenses enumerated in Titles 8, 18, 19, 21, and 31 of the United States Code and other related offenses.

6. Based on my training and experience and the facts set forth in this affidavit, I respectfully submit that there is probable cause to believe that evidence of violations 18 U.S.C. §

2251 (production of child pornography) and 18 U.S.C. § 2252(a)(4)(B) (possession of child pornography), will be discovered on the SUBJECT DEVICES described in Attachment A.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

7. The SUBJECT DEVICES to be searched, further described in Attachments A.1, A.2, and A.3, are three cellular phones: (1) a black Samsung Galaxy S5 cellular phone (Model SM-G900A), (2) a gold Samsung Galaxy S7 (IMEI 359754071653702), and (3) a black Apple iPhone (IMEI 358689094665260). The SUBJECT DEVICES are currently in law enforcement possession, located at Pennsylvania State Police (“PSP”) Computer Crimes, Fogelsville barracks.

8. The applied-for warrant would authorize forensic examination of the SUBJECT DEVICES for the purpose of identifying electronically stored data, more particularly described in Attachment B.

JURISDICTION

9. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is a “district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

APPLICABLE LAW

10. Title 18, United States Code, Section 2251(a) states:

Any person who employs, uses, persuades, induces, entices, or coerces any minor to engage in, or who has a minor assist any other person to engage in, or who transports any minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, shall be punished as provided under subsection (e), if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was

produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed.

Title 18 U.S.C. § 2252(a)(4)(b) states:

Any person who . . . knowingly possess, or knowingly accesses with intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means, including by computer, if—(i) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and (ii) such visual depiction is of such conduct; shall be punished as provided in subsection (b) of this section.

11. Based on my knowledge, training, and experience, court records, and information provided by investigators with prior experience investigating VASQUEZ-BARRIOS, I submit that probable cause exists to search the SUBJECT DEVICES described in Attachment A for evidence of violations of 18 U.S.C. §§ 2251(a) and 2252(a)(4)(B).

DEFINITIONS

12. The following definitions apply to this Affidavit and Attachment B:

a. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

b. “Computer,” as used herein, refers to “an electronic, magnetic, optical,

electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

c. “Wireless telephone:” A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

d. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

e. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, digital, or magnetic form.

f. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or

simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person. An image can depict the lascivious exhibition of the genitals or pubic area even if the child is clothed, *see United States v. Knox*, 32 F.3d 733 (3d Cir. 1994), *cert. denied*, 513 U.S. 1109 (1995); *United States v. Caillier*, 442 F. App'x 904 (5th Cir. 2011), so long as it is sufficiently sexually suggestive under the factors outlined in *United States v. Dost*, 636 F. Supp. 828 (S.D. Cal. 1986), *aff'd sub nom, United States v. Wiegand*, 812 F.2d 1239 (9th Cir. 1987), *aff'd*, 813 F.2d 1231 (9th Cir. 1987), *cert. denied*, 484 U.S. 856 (1987)

g. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

PROBABLE CAUSE

13. On or around October 20, 2023, the Bethlehem Township Police Department was dispatched to St. Luke's Hospital, Fountain Hill campus, for a report of a sexual assault of a six-year-old female. The minor female victim (herein "MFV1") verbally disclosed in the early morning to her mother (herein "AV") that "Tio Gerb came into my room and touched me." AV stated to law enforcement that "Tio Gerb" is AV's brother, Gerber VASQUEZ-BARRIOS. AV stated to law enforcement that VASQUEZ-BARRIOS cohabitates with AV and MFV1.

14. AV stated to law enforcement that MFV1 stated that MFV1 was sleeping when VASQUEZ-BARRIOS climbed over top of her and put his hands down her pajama pants and touched her.

15. On or around November 7, 2023, a forensic interview was conducted at the John van Brakle Child Advocacy Center in Allentown, Pennsylvania. Forensic Interviewer (“FI”) Allyce Brailo conducted the interview. MFV1 stated to FI Brailo that MFV1 had to go to the hospital to check “where it hurts.” When asked where it hurt, MFV1 pointed to her inner thigh and her vagina. MFV1 stated that someone, who she later identified as her uncle, Tio Gerber, touched her where they weren’t supposed to. MFV1 stated that “she was sleeping” and she “didn’t like it.” MFV1 pointed to her vagina and inner thighs multiple times throughout the interview when recalling where VAZQUEZ-BARRIOS touched her. MFV1 stated that VASQUEZ-BARRIOS first touched her on her thigh and used the flashlight on his phone to check if she was awake. MFV1 stated that VASQUEZ-BARRIOS put his cell phone in his pocket and then started touching her vagina with his hand. MFV1 also stated that when VASQUEZ-BARRIOS finished, “he was on his phone” and “was watching something.” MFV1 stated that VASQUEZ-BARRIOS did not show her what he was watching and that he had the volume turned down. In my training and experience, pertaining to the use of cellular devices for capturing video, cellular devices that are recording video in a dark area will utilize the device’s flashlight in the same manner that a camera utilizes its flash, to illuminate the area. Furthermore, the screen that is facing the operator of the cellular device will be illuminated, giving the appearance that the operator is “watching something.”

16. On or around November 17, 2023, VASQUEZ-BARRIOS was arrested for Pennsylvania state charges of Aggravated Indecent Assault (F1), Corruption of Minors (F3), and Indecent Assault (M1) in relation to his sexual abuse of MFV1. This case remains pending in the Northampton County Court of Common Pleas.

17. VASQUEZ-BARRIOS was arrested at his place of employment, Hotel Bethlehem, in Northampton County, Pennsylvania. Upon a search incident to arrest of VASQUEZ-BARRIOS's person, a black Apple iPhone (IMEI 358689094665260) was found and seized as evidence. After obtaining search warrant BT-2023-2473, issued by a judge of the Northampton County Court of Common Pleas, the iPhone was sent to PSP Computer Crimes for forensic analysis. At the time of his arrest, VASQUEZ-BARRIOS also had a backpack containing his personal effects. VASQUEZ-BARRIOS chose not to bring the backpack with him to detention and instead left the backpack with law enforcement. The backpack was inventory searched at Bethlehem Township Police Department. Upon inventory search, two (2) additional cellular phones were discovered and seized as evidence. Pursuant to search warrants BT-2023-2477 and BT-2023-2476, issued by a judge of the Northampton County Court of Common Pleas, the additional cellular phones, described as a gold in color Samsung Galaxy S5 (Model SM-G900A) and black in color Samsung Galaxy S7 (IMEI 359754071653702), were also sent to PSP Computer Crimes for forensic analysis. The Samsung S5 and S7 did not have any battery life at the time of discovery. In my training and experience, older cellular phones can be used as storage devices for digital contraband. Keeping older devices, such as cellular phones, close in proximity is indicative that there may be something important to the owner stored on such devices.

18. The SUBJECT DEVICES remained in the custody of Bethlehem Township Police Department until they were turned over to an HSI Task Force Officer at PSP Computer Crimes in Fogelsville, Pennsylvania. Based on my training and experience and information relayed to me by other law enforcement officers, I know that the SUBJECT DEVICES have been stored in a manner in which the contents are, to the extent material to this investigation, in substantially

the same state as they were when the SUBJECT DEVICES first came into law enforcement's possession.

19. On or around January 3, 2024, Bethlehem Township Police Department received a phone call from VASQUEZ-BARRIOS's ex-wife (herein "YGR"). YGR told law enforcement that YGR shares two biological daughters with VASQUEZ-BARRIOS. YGR stated that her oldest daughter (herein "MFV2") disclosed that her father, VASQUEZ-BARRIOS, touched MFV2 inappropriately and that YGR would like to file a police report. MFV2 was 15 years old at the time of the report.

20. During the forensic interview of MFV2, MFV2 recalled an incident that she says occurred in December 2022 or January 2023, when MFV2 was 14 years old. MFV2 states that she and her dad VASQUEZ-BARRIOS were playing "i-Message" games late at night. MFV2 stated that she was upstairs in her cousin's bedroom at the time and her dad was downstairs in his bedroom. MFV2 stated that VASQUEZ-BARRIOS asked MFV2 if she wanted to play a game. MFV2 stated that this gave her "a bad feeling in her stomach."

21. A short time later, MFV2 and her minor female cousin went downstairs to VASQUEZ-BARRIOS's bedroom after he asked MFV2 to come down to talk. MFV2 saw that her nine-year-old sister, CV, was asleep in VASQUEZ-BARRIOS's bed at the time.

22. VASQUEZ-BARRIOS encouraged MFV2's cousin to go back upstairs and once she left, told MFV2 to close the door to the bedroom. MFV2 stated that she felt uncomfortable being alone with VASQUEZ-BARRIOS, but kept telling herself: "He's my dad, he's not going to do anything to me, he's not going to hurt me, he's my dad, like if he does stuff to other people, he's not going to do it to me because I'm his daughter." Earlier in the interview, MFV2 had stated that several years earlier she woke up during the night and saw VASQUEZ-BARRIOS's

hand under a blanket, and it looked like he was touching MFV2's minor female friend, who was in bed with MFV2 while sleeping over.

23. MFV2 stated that the conversation with VASQUEZ-BARRIOS started off normal. MFV2 stated that the conversation changed, and VASQUEZ-BARRIOS began asking her sexual questions. MFV2 stated that VASQUEZ-BARRIOS asked if MFV2 had ever done anything sexual or intimate with her boyfriend. MFV2 stated that she kept trying to change the subject to other things, but VASQUEZ-BARRIOS would just return to asking sexual questions. MFV2 stated that she was uncomfortable and shaky.

24. MFV2 stated that she was standing, and VASQUEZ-BARRIOS was laying in his bed and MFV2 could see that VASQUEZ-BARRIOS was touching himself. Initially, VASQUEZ-BARRIOS was covered by a blanket, but MFV2 stated that she could see his hand near his midsection. MFV2 stated that she wanted to leave, was very uncomfortable, and was trying to pretend that she couldn't see what VASQUEZ-BARRIOS was doing.

25. MFV2 stated that VASQUEZ-BARRIOS kept asking inappropriate questions. MFV2 stated that when she told VASQUEZ-BARRIOS that she didn't know the answer, VASQUEZ-BARRIOS said to her, "why don't you just show me." MFV2 demonstrated how VASQUEZ-BARRIOS grabbed her and pulled her arm/hand toward him. MFV2 stated that VASQUEZ-BARRIOS was trying to force her hand onto his privates/penis. MFV2 stated that she kept saying stop and trying to pull away, eventually yelling "Papi stop!" MFV2 stated that she kept saying "can you stop, can you stop" and VASQUEZ-BARRIOS kept pulling. MFV2 stated that VASQUEZ-BARRIOS kept saying "c'mon [MFV2 nickname] c'mon." MFV2 stated that she tried to pull away harder than she had ever tried to pull away in her life. MFV2 stated that VASQUEZ-BARRIOS finally let go because she was not going to stop pulling. MFV2

stated that when VASQUEZ-BARRIOS finally let go, VASQUEZ-BARRIOS said “okay [MFV2 nickname] just go upstairs.”

26. MFV2 stated that while a blanket was originally covering VASQUEZ-BARRIOS’s pelvic area, eventually his penis and his hand touching it were exposed. MFV2 stated that VASQUEZ-BARRIOS’s penis “was out” and he was “touching it, like, softly” while asking her questions. MFV2 stated that VASQUEZ-BARRIOS’s hand was on his penis and he was moving his hand “up and down . . . slowly.” MFV2 explained that VASQUEZ-BARRIOS’s penis looked like the end of a broomstick.

27. MFV2 stated that when she got upstairs to her cousin’s room, MFV2 really wanted to talk about what had just happened, but felt like it would be her fault. MFV2 stated that she had to act like nothing happened.

28. As a result of this incident, VASQUEZ-BARRIOS was arrested and charged with Pennsylvania state charges of Corruption of Minors (F3), Indecent Assault by Forceable Compulsion (M1), and Endangering the Welfare of Children (M1) in relation to his exploitation of MFV2. This case remains pending in the Northampton County Court of Common Pleas.

29. During the forensic interview of MFV2, she stated that VASQUEZ-BARRIOS had images on his Apple iPhone cell phone of a minor female friend of MFV2 (herein “MFV3”). This is the same minor female who MFV2 believes VASQUEZ-BARRIOS was touching when she woke up in the middle of the night during a sleepover. MFV2 stated that VASQUEZ-BARRIOS would invite MFV3 to sleep over when YGR was not home.

30. MFV2 stated that VASQUEZ-BARRIOS did not want her looking around on his phone, but in one instance MFV2 accidentally clicked a button on VASQUEZ-BARRIOS’s cell phone and saw a photo gallery. MFV2 stated that she saw a “ton” of photos of her friend,

MFV3, taken while MFV3 was sleeping. MFV2 stated that the photos were all taken in VASQUEZ-BARRIOS's bedroom at MFV2's maternal grandmother's house. MFV2 stated that MFV3's clothes were on in the pictures and that MFV3's mouth was open.

31. MFV2 stated that she recalled seeing images on VASQUEZ-BARRIOS' phone where VASQUEZ-BARRIOS's "thumb" was in the picture and MFV3 was sleeping. MFV2 stated that knowing what MFV2 knows now, MFV2 does not believe it was VASQUEZ-BARRIOS's thumb, but rather his penis. MFV2 stated that the last photograph she saw was VASQUEZ-BARRIOS standing above MFV3 and it looked like VASQUEZ-BARRIOS's penis may have been exposed in the bottom of the picture. MFV2 stated that initially she thought it may have been VASQUEZ-BARRIOS's finger, but now MFV2 doesn't think it was a finger. MFV2 stated that VASQUEZ-BARRIOS was standing in all the pictures.

32. On May 20, 2024, a forensic interview was conducted at the HSI RAC Allentown office in Allentown, Pennsylvania, with MFV3. MFV3 was identified following the forensic interview of MFV2 and "CV," Gerber VASQUEZ-BARRIOS' biological daughters. MFV3 is a peer of MFV2, the older of VASQUEZ-BARRIOS' daughters.

33. HSI FI Denise Wilson conducted the forensic interview with MFV3. MFV3 stated that she is 15 years old and in the 9th grade. FI Wilson showed MFV3 a picture that was found on a cell phone attributed to VASQUEZ-BARRIOS that was searched by Bethlehem Township Police Department pursuant to a search warrant. MFV3 confirmed that the picture was of her sleeping when she was between 9 and 10 years old. MFV3 stated that she knows where the picture was taken and stated that the picture may have been taken by CV and MFV2's dad.

33. MFV3 stated, “I had their dad’s [VASQUEZ-BARRIOS’s] number, and he used to text me.” MFV3 stated that on one occasion, she texted VASQUEZ-BARRIOS because she was going to sleep over and wanted to know when MFV2 and CV would be home. VASQUEZ-BARRIOS invited her over even though MFV2 and CV were not home at the time. MFV3 stated that VASQUEZ-BARRIOS was in MFV3’s phone under the contact “[MFV2] and [CV’s] Dad.” MFV3 stated that she no longer has the cell phone she used to communicate with VASQUEZ-BARRIOS, as this occurred years prior.

35. MFV3 stated that she did not know VASQUEZ-BARRIOS’s name but stated that he had a “Giants themed room.” I have reviewed images of the bedroom attributed to VASQUEZ-BARRIOS and confirmed that there are New York Giants decorations and memorabilia present in the bedroom.

36. MFV3 stated that there was a time when VASQUEZ-BARRIOS would text MFV3 “all the time” and that MFV3 would block him. MFV3 stated that she would “try to avoid it” (communicating with VASQUEZ-BARRIOS) as much as possible. MFV3 stated that as she got older, she stopped being friends with MFV2, but that VASQUEZ-BARRIOS would still text MFV3. MFV3 stated that she began to realize that it was weird. MFV3 stated “He’s an adult and I’m a kid … this is shady.”

37. MFV3 stated that the picture shown to her was likely taken during a sleepover when MFV3, MFV2, and CV slept in VASQUEZ-BARRIOS bed and VASQUEZ-BARRIOS slept on the floor next to the bed. MFV3 stated that she believed she only slept in VASQUEZ-BARRIOS’ bed one time and went on to describe that one time. MFV3 stated that the three girls (CV, MFV2, and MFV3) were all playing on their phones before bed. MFV3 stated that VASQUEZ-BARRIOS was also playing video games. MFV3 stated that she woke up in the

middle of the night and saw VASQUEZ-BARRIOS was doing something to himself. MFV3 stated: "it's nasty. [VASQUEZ-BARRIOS] was touching his private parts with his hand." MFV3 stated that VASQUEZ-BARRIOS was laying down, but there was movement: "I opened my eyes and saw it. It was disgusting so I turned over and closed my eyes and went to sleep." MFV3 stated that VASQUEZ-BARRIOS was on the floor when he was touching his private parts. MFV3 stated that VASQUEZ-BARRIOS had a blanket over top of him. MFV3 stated "I think he saw that I woke up and he stopped. Not really sure because I was a kid."

38. MFV3 stated that VASQUEZ-BARRIOS would never call MFV3, only text, through messages. MFV3 stated that she did not communicate with VASQUEZ-BARRIOS through Snapchat or other social media applications. MFV3 stated that, at the time, she had an Android or iPhone SE. MFV3 stated that she believes VASQUEZ-BARRIOS had an iPhone, but she was not sure. MFV3 stated that she thinks VASQUEZ-BARRIOS would take pictures and/or videos of CV and MFV2, but that MFV3 doesn't remember VASQUEZ-BARRIOS taking pictures of MFV3.

39. During the investigation, VASQUEZ-BARRIOS' ex-wife, YGR, has communicated with law enforcement regarding VASQUEZ-BARRIOS's former employment at KidsPeace. According to YGR, VASQUEZ-BARRIOS was employed at KidsPeace, specifically the "Kids Haven" program, which provided residence to unaccompanied minor children following encounters with immigration. YGR stated to law enforcement, in sum and substance, that VASQUEZ-BARRIOS had regular contact with minors in his job at KidsPeace and that YGR had discovered hand-written "love" letters, which she believed were authored by a minor. YGR shared those letters with law enforcement. I have reviewed those letters and found that the author identified himself as "17 years old" and that the letters contain discussions of a romance

between VASQUEZ-BARRIOS and the minor. The minor has not been identified by law enforcement. The letters are written in the Spanish language and have been translated utilizing open-source translation services and Spanish speaking law enforcement.

40. Some excerpts from the letters include the following:

- “I like you too, but no one can know that.”
- “I want to kiss you, hug you, and well, do everything with you.”
- “A boy sent me a letter You should know that I’m not interested in that boy ok. I love you only and not those boys.”
- “You look very handsome as always love. I love you so much daddy.”
- “I swear that when I get out of here I will wait for you. Love kisses daddy.”
- “Gerber When I look at you I want to kiss you I’m being bad, please, I just don’t like that they’re looking at you like Melinda.”
- “I had a good time today although we can’t talk alone I wanted to kiss you and if it was our secret I didn’t tell anyone about this.”
- “I love you and I hope you are sincere with me. I love you and you are only mine. Do not worry about that phone thing. If I am with you I will not open the phone or anything ok.”
- “I hope you’re not married and you want something serious with me not just to play with me Don’t pay attention to what the boys say. I’m drooling over you You kiss so well it’s a pity we can’t kiss here baby.”
- “Look, I will talk to my family about you I know that I am 17 years old, but I do not care I want to be yours forever daddy.”

41. As a result of the information shared by YGR, I sent a subpoena to KidsPeace Corporation General Counsel Andrew Burke on or around June 13, 2024, requesting records related to the employment of VASQUEZ-BARRIOS and any misconduct recorded during that employment. On or around July 1, 2024, General Counsel Burke informed me that VASQUEZ-BARRIOS was employed from 10/7/13 through 11/22/16. During that time, VASQUEZ-BARRIOS worked for the KidsHaven program, which provided short-term shelter and care for unaccompanied children through the Department of Health and Human Services’ Office of Refugee Resettlement (“ORR”).

42. According to the ORR website, “an unaccompanied child (UC) has no lawful immigration status in the United States, is under 18 years of age, and has no parent or legal

guardian in the United States or no parent or legal guardian in the United States is available to provide care and physical custody.” Further, “[t]he age of these individuals, their separation from parents and relatives, and the hazardous journey they take make UC especially vulnerable to human trafficking, exploitation, and abuse.”

43. At the time of his termination, VASQUEZ-BARRIOS was employed as a “Youth Care Worker II,” responsible for providing direct supervision of UCs. Per a notification letter dated December 1, 2016, to VASQUEZ-BARRIOS from “Tina,” Employee Relations Representative, VASQUEZ-Barrios was terminated for “violation of the KidsPeace Boundaries Between Staff and Clients Policy.” The notification further states “you are no longer permitted on KidsPeace property … and you are prohibited from contacting any KidsPeace clients.”

44. According to a KidsPeace “Request for Termination Form,” VASQUEZ-Barrios was involved in an incident on November 22, 2016. The incident is described as a “Violation of Company Policy or Procedures” and a “Boundary Violation.” The form describes an incident in which VASQUEZ-BARRIOS provided his phone number to a female UC after inquiring as to whether she had a boyfriend. As a result of this incident, VASQUEZ-BARRIOS was placed on administrative leave and, after an inquiry, ORR requested his termination “due to potential threat of trafficking.”

45. The investigation into VASQUEZ-BARRIOS reveals a pattern of inappropriate behavior with minors. VASQUEZ-BARRIOS was frequently entrusted with caring for minor children, through family members and professionally, and repeatedly abused his position of trust and authority by acting inappropriately with minor females. Further, the facts herein demonstrate that on numerous occasions, VASQUEZ-BARRIOS utilized devices, believed to include the SUBJECT DEVICES, to communicate with minors and to further those inappropriate

behaviors, including to record and store visual depictions of minor children sleeping and to produce child pornography as defined in 18 U.S.C. § 2256(8).

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

46. As described in Attachment B, this application seeks permission to search for images, videos, and records that might be found on the SUBJECT DEVICES, in whatever form they are found. One form in which these items might be found is data stored on a computer's hard drive, mobile device, or other storage media. Thus, the warrant applied for would authorize the seizure of electronic devices and electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

47. I submit that there is probable cause to believe those records will be stored on the SUBJECT DEVICES, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

48. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on the SUBJECT DEVICES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image

files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic

programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

49. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to

know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

d. Furthermore, the electronic media may contain contraband, in the form of images and videos depicting the sexual exploitation of minors.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO ENGAGE IN THE SEXUAL EXPLOITATION OF CHILDREN

50. Based on my education, training, and experience, as well as information obtained from other experience law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who engage in the sexual exploitation of children:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including, but not limited to digitized/electronic media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. In some instances, these depictions show the individual's own sexual activity with children. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected

child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain their child pornographic material in the privacy and security of their home or some other secure location.

Individuals who have a sexual interest in children or images of children typically retain this material for many years.

d. Likewise, such individuals often maintain their child pornography collections in a digital or electronic format in a safe, secure and private environment, such as a computer, cell phone, or other electronic storage devices (e.g., hard drives or USB drives). These collections are often maintained for years and are kept close by, usually at the individual's residence, inside the individual's vehicle, or, at times, on their person, to enable the individual to view the collection, which is valued highly. Although it is possible, a person who has this type of material is not likely to destroy the collection, including during moves.

e. Such individuals also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

g. Such individuals frequently retain records of their child exploitation and child

pornography activities for long periods of time, particularly when they are involved in ongoing criminal conduct. Offenders who engage in child exploitation and child pornography often do so for extended periods of time spanning years, and due to the nature of the crime retain evidence and records of their activities for many years. Based on my experience, the passage of long periods of time will not remove the possibility that the evidence of the crimes will still remain. The evidence may also be innocuous at first glance (e.g., financial, credit card and banking documents, travel documents, receipts, documents reflecting purchases of assets, personal calendars, telephone and address directories, check books, videos and photographs, utility records, ownership records, letters and notes, tax returns and financial records, escrow files, telephone and pager bills, keys to safe deposit boxes, packaging materials, computer hardware and software), but have significance when considered in light of other evidence. These persons may no longer realize they still possess the evidence or may believe law enforcement could not obtain a search warrant to seize the evidence. These persons may also be under the mistaken belief that he/she has deleted, hidden or further destroyed any computer-related evidence, but this information may be retrievable by a trained forensic computer expert.

h. Individuals involved in child exploitation and child pornography and/or their associates frequently take, or cause to be taken, photographs or videos of themselves, their associates, their property, and their product, and maintain those photographs or videos in their residences and within computer and electronic equipment in their residences.

i. These persons frequently maintain listings of names, aliases, telephone numbers, pager numbers, facsimile numbers, physical addresses, and email addresses, sometimes

encoded and sometimes not encoded, for the purpose of contacting their victims or co-conspirators, and these records are typically maintained on their person or in their residences, stash houses, businesses, and/or vehicles, so they are readily available in order to efficiently conduct their child exploitation-related activities. Moreover, such records are often stored electronically within the memory of telephones, computers, and/or personal digital assistants such as iPhone, Android and other electronic devices.

j. Individuals involved in child exploitation and child pornography frequently utilize cellular telephones, satellite telephones, pagers and text messaging devices, voicemail or answering machine systems, telephone calling cards, computers, email, and/or personal digital assistants such as “smart” phones in order to communicate with their victims or co-conspirators, and these items are often maintained on their person or in their residences, stash houses, businesses, and/or vehicles where they are readily available. A cellular telephone’s memory may contain the telephone number that is assigned to that telephone (which will enable investigators to retrieve records concerning that telephone and analyze those records). In addition, cellular telephones often have internal logs which record the outgoing and incoming calls, including the numbers associated with those calls, and this information can also assist in identifying victims or co-conspirators. Similarly, cellular telephones are commonly used for text messages or other forms of electronic messages and often store the messages, and these messages may provide insight into the (a) the nature, extent and methods of child exploitation activities and operations of the conspirators; (b) the identities and roles of co-conspirators; (c) the distribution and transfer of photographs, images, videos, and other records involved in those activities; (d) the existence and location of records; (e) the location and source of

resources used to finance their illegal activities; and (f) any attempt to hide the identity or location of those involved. In addition, the information in a phone's memory may constitute admissible evidence of the commission of child exploitation-related offenses. Cellular telephones, computers and other electronic storage devices may also include an address book, calendar and lists of frequently called telephone numbers which may help establish the identities of other individuals who are in frequent contact with the user and involved in child exploitation-related activities. These devices may also include photographs, video recordings and other records of the type described above. Based on my training and experience, I know that even though individuals involved in child exploitation and child pornography will discontinue use of a telephone, they will sometimes keep the physical phone in their possession.

k. Non-pornographic, seemingly innocuous images of minors are often found on media belonging to child exploitation offenders. Such images are useful in attempting to identify actual minors depicted in child pornography images, or who were otherwise exploited by the offender, that are found during the execution of a search warrant. In certain cases, such images may also assist in determining the origins of a particular child pornography image or series of images, or the location of the offender's contact with the minor.

51. I have reason to believe that VASQUEZ-BARRIOS shares the above characteristics common to individuals who sexually exploit children, including those who use the Internet and electronic devices to produce, possess, and access with intent to view child pornography, based on the following: As further detailed herein, there is probable cause to believe that VASQUEZ-BARRIOS sexually assaulted MFV1 in her home and possibly filmed that

conduct; VASQUEZ-BARRIOS attempted to force sexual contact on MFV2; and VASQUEZ-BARRIOS takes and stores photographs of underage females, including MFV3 while she was sleeping and VASQUEZ-BARRIOS's penis was exposed.

TIME OF SERVICE REQUEST

52. As mentioned above, the SUBJECT DEVICES are currently in the lawful possession of law enforcement as they were seized during the arrest of VASQUEZ-BERRIOS. Therefore, the execution of the requested warrants will not involve the physical intrusion on the premises of a civilian or other individual. Accordingly, I submit that good cause exists to permit law enforcement to execute the requested warrants at any time of day or night.

CONCLUSION

53. Based upon the information above I respectfully submit that there is probable cause to believe that violations of Title 18 U.S.C. Sections 2251 and 2252 have been committed and that evidence of those violations is located on the SUBJECT DEVICES seized from VASQUEZ-BARRIOS' person during arrest. This evidence, listed in Attachment B to this affidavit, which is incorporated herein by reference, is contraband, the fruits of crime, or things otherwise criminally possessed, or property which is or has been used as the means of committing the foregoing offenses. Therefore, I respectfully request that the attached warrant be issued authorizing the search and seizure of the SUBJECT DEVICES identified in Attachment A, for the items listed in Attachment B.

Respectfully submitted,

/s/ Sean R. Crawford
Sean R. Crawford
Special Agent
Homeland Security Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on December 6, 2024.

HONORABLE PAMELA A. CARLOS
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A.1

DESCRIPTION OF ITEMS TO BE SEARCHED

Black in color Samsung Galaxy S5 cellular phone (Model SM-G900A)



ATTACHMENT A.2

DESCRIPTION OF ITEMS TO BE SEARCHED

Gold Samsung Galaxy S7 (IMEI 359754071653702)



ATTACHMENT A.3

DESCRIPTION OF ITEMS TO BE SEARCHED

Black Apple iPhone (IMEI 358689094665260)



ATTACHMENT B

EVIDENCE TO BE SEARCHED FOR AND SEIZED

Evidence of violations of 18 U.S.C. Sections 2251 and 2252 including the following:

1. All visual depictions of minors engaged in sexually explicit conduct produced using minors engaged in such conduct.
2. All documents in electronic form, and, any other electronic data or other memory features pertaining to the possession, receipt, access to, or distribution of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, or pertaining to an interest in child pornography or minors whether transmitted or received, or which tends to show the knowing possession of any child pornography possessed.
3. All records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission in or affecting interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.
4. All records which evidence operation or ownership or use of computer or electronic equipment or devices, including, but not limited to, correspondence, sales receipts, bills, financial records, tax records, personal photographs, telephone records, notebooks, diaries, reference materials, or other personal items, and registration information for any software on the computer or device.
5. All computer or electronic device passwords, keywords and other data security devices designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software, or other programming code. Any password or encryption key that may control access to a computer/phone operating system, individual computer/phone files, or other electronic data.